LAUREA
UNIVERSITY OF APPLIED SCIENCES
Prime Mover

Tietoturvapolitiikan luominen pk-yritykselle

Santasalo, Matti

2014 Laurea UAS, Leppävaara

Laurea University of Applied Sciences
Leppävaara

Tietoturvapolitiikan luominen pk-yritykselle

Matti Santasalo
Degree Programme in Business information technology
Bachelor's Thesis
5, 2014

Laurea University of Applied Sciences **Abstract**
Leppävaara
Bachelor's Degree Programme in Business Information Technology

Santasalo, Matti

Creating an information security policy for a SMB

Year 2014 Pages 31

This study consists of the process of making an information security policy for a small medium sized company. The study progressed as a real-estate company wanted to improve their level of information security. This study used a constructive research method, where the goal is to solve some kind of problem based on a wide range of theoretical information and empirical evidence about the subject of improvement. The goal was to create an information security policy for the company. The result of this research became the information security policy which works for a basis for the systematical improvement for the company.

Key words, Information Security policy, Constructive research, BSI, MIS, 27002, Information security analysis

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Santasalo, Matti

Tietoturvapolitiikan luominen Pk-Yritykselle

Vuosi 2014 Sivumäärä 31

Tämä opinnäytetyö käsittelee tietoturvapolitiikan laatimisesta Pk-yrityksen tarpeisiin. Tutkimus sai alkunsa erään kiinteistönvälitysliikkeen halusta parantaa omaa tietoturvaansa. Tutkimuksessa käytettiin konstruktiivista tutkimusmenetelmää jossa tarkoituksena on ratkaista jokin ongelma. Koska tietoturvan kehittämisen kannalta kaikkein olennaisin dokumentti eli tietoturvapolitiikka puuttui yritykseltä, tuli se luoda käyttäen apuna syvällistä teoreettista tietoa, sekä käytännön empiiristä tietoa tutkimuksen ja kehittämisen kohteesta. Tutkimuksen tuloksena, eli konstruktiona syntyi tietoturvapolitiikka joka toimii pohjana yrityksen tietoturvan systemaattiselle kehittämiselle.

Avainsanat: Tietoturvapolitiikka, Konstruktiivinen, Tietoturva, BSI, MIS, 27002, Johtaminen, Strateginen, Tietoturva, Tietoturva-analyysi

Table of Contents

1 Johdanto

Tämän päivän yritykset ovat jatkuvasti tekemisissä tietoturvan kanssa. Tietojärjestelmien ja palvelujen jatkuva digitalisoituminen tuo yrityksille velvollisuuksia huolehtia asiakkaidensa, yhteistyökumppaniensa ja henkilöstönsä yksityisyydensuojasta, jossa tietoturvallisuus korostuu entisestään. Tiedon määrä kasvaa koko ajan yhä kiihtyvällä tahdilla, joka tuo mukanaan mahdollisuuksia, mutta myös uhkia. Tietoturvasta huolehtiminen on nähtävä pitkäaikaisena prosessina, johon kuuluu muutoksia ja kehityksen seuraamista ja jossa kytkennät yrityksen liiketoimintastrategiaan tulee ottaa huomioon. Yrityksen täytyy pysyä muutoksen vauhdissa mukana ja osata ennakoida liiketoiminnan tarpeet tarpeeksi pitkälle aikavälille. (Andreasson & Koivisto, 2013, s.11-12)
Tämän opinnäytetyön tavoitteena on pyrkiä luomaan tietoturvapolitiikka vastaamaan pk-yrityksen tarpeita. Lukija tullaan tutustuttamaan tietoturvaa koskeviin eri aihe-alueisiin, jotta myös sellainen henkilö, jolle tietoturva ei ole ennestään tuttu aihe, voi ymmärtää niiden merkityksen. Opinnäytetyön tekemisessä käytetään hyväksi ns. konstruktiivista tutkimusmenetelmää. Tutkimusmenetelmän ajatuksena on määrittää mielekäs ongelma ja laatia sille ratkaisu käyttäen hyväksi syvällistä teoreettista pohjaa, sekä käytännön työstä luotua empiiristä tietoa. (Ojasalo, Moilanen, Ritalahti, 2009)

Työ koostuu teoria- ja käytännön osuudesta, jossa teoriaosuudessa käydään läpi tietoturvapolitiikan luomisprosessiin tarvittavaa taustatietoa. Käytännön osuudessa kohdeyritykselle tehdään nykyisen tietoturvatason analyysi, joka toimii pohjana itse tietoturvapolitiikan luomiselle. Tietoturvapolitiikan laatiminen jatkuu johdon ja työntekijöiden haastatteluilla eri tietoturvapolitiikan aiheita koskeviksi.

Opinnäytetyön tekijänä toimii Laurea ammattikorkeakoulun tietojenkäsittelyn opiskelija, joka työskenteli 8kk ajanjakson aikana kohteena olevan yrityksen kanssa tavoitteena parantaa yrityksen tietoturvaa. Koska tietoturva on aihealueena varsin laaja, tuli tutkimusaihetta rajata pienemmäksi ja näin aiheeksi lopulta muodostui organisaation tietoturvasuunnitelman kannalta keskeinen osa, tietoturvapolitiikan luominen. Yrityksen yhteyshenkilönä toimi hallintojohtaja, joka oman toimensa ohella toimii myös yrityksen tietohallintovastaavana, sekä toimitusjohtaja. Tutkimus perustuu opinnäytetyöntekijän tekemiin selvityksiin ja havaintoihin yritysympäristössä osallistumalla yrityksen jokapäiväiseen liiketoimintaan, sekä yrityksen johdon, tietohallintovastaavan ja yrityksen työntekijöiden haastatteluihin.

Kohdeyritys on pieni kiinteistönvälitystä harjoittava yritys, joka työllistää kuusi henkilöä. Toimipisteitä on yksi joka sijaitsee Espoossa ja sen asiakkaita ovat pääasiassa yksityiset ihmiset, jotka haluavat joko myydä tai ostaa asunnon tai kiinteistön. Yrityksen liiketoimintastrategiana on tuottaa laadukkaita, luotettavia ja yksilöllisiä kiinteistönvälitys-palveluita asiakkailleen. Yritys tavoittelee tyytyväisiä asiakkaita ja pitkäkestoisia asiakas-

suhteita. Yritys ei kilpaile halvalla hinnalla vaan pyrkii löytämään ne asiakkaat jotka ovat valmiita maksamaan laadusta ja turvallisuudesta.

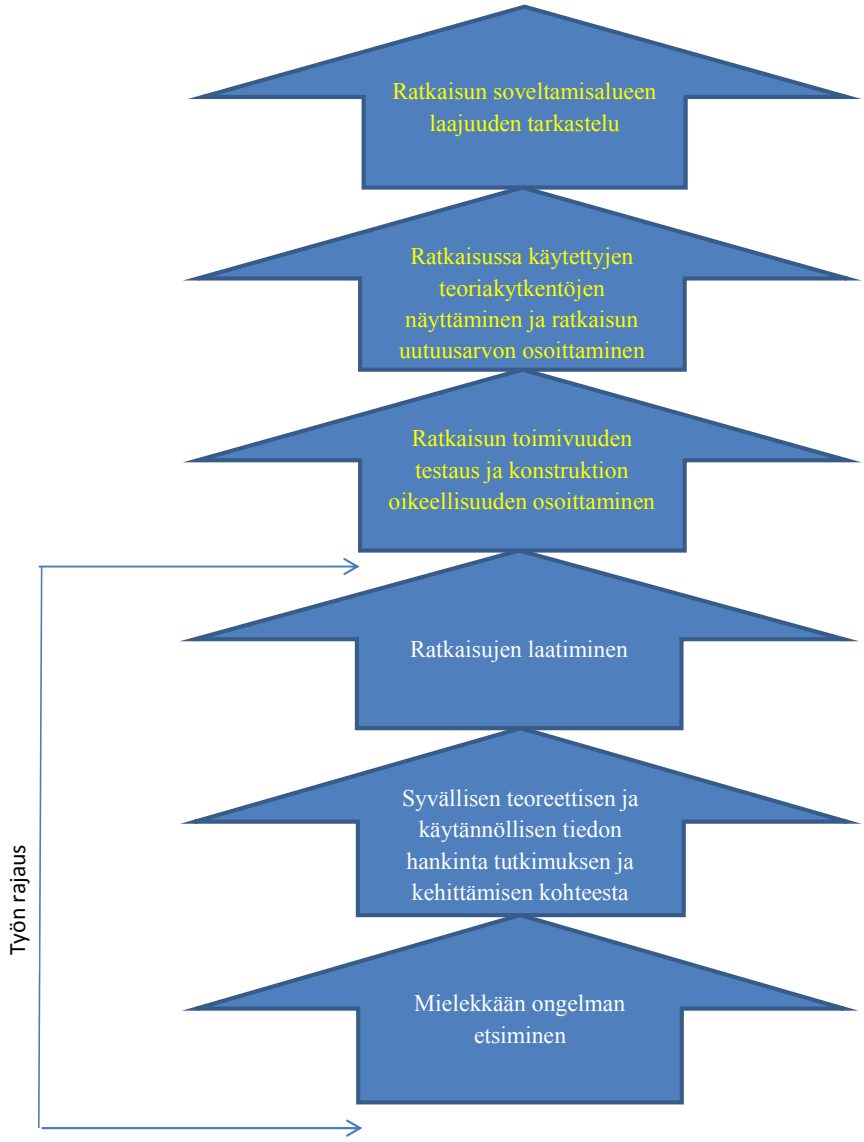
2 Tutkimuksen ongelma ja tutkimusmenetelmän valinta

Tutkiessani alan teoreettista tietoa, tutkimusongelmakin kävi monipiirteisemmäksi. Koska tietoturvapolitiikka toimii ohjenuorana kaikille muille yrityksen tietoturvaan liittyville linjauksille sekä ohjeille, tutkimusongelmana voitiin pitää tietoturvapolitiikan puuttumista. Tärkeää oli myös määrittää yrityksen haluttu tietoturvan taso, jotta se vastaisi mahdollisimman hyvin yrityksen todellisia tarpeita ja olisi oikeassa suhteessa käytettävissä oleviin resursseihin.

Opinnäytetyössä käytettiin konstruktiivista tutkimusmenetelmää, joka koostuu monipuolisista tiedonkeruumenetelmistä, kuten haastatteluista, kyselyistä, ryhmäkeskusteluista ja havainnoinnista. Ojasalo, Moilanen ja Ritalahti painottaa, että konstruktiivinen lähestymistapa ei sinänsä rajaa pois mitään menetelmää, vaan tutkimuksessa on tyypillistä juuri menetelmien kirjavuus. Tutkimuksessa on haettu tietoa alan kirjallisuudesta, artikkeleista, standardeista ISO IEC 27001 ja 27002, BSI-katalogista, sekä valtiovarainministeriön tietoturvaohjeista, jotka perustuvat alan standardeihin.

Konstruktiivisessa tutkimuksessa yhdistyy aiempi teoreettinen tieto, sekä käytännön työstä syntyvä empiirinen tietämys. Lähestymistapana konstruktiivinen tutkimus soveltuu, erittäin hyvin sellaisiin tutkimuksiin jossa tavoitteena on luoda jokin konkreettinen tuotos eli konstruktio, esimerkiksi järjestelmä, malli tai suunnitelma. (Ojasalo, Moilanen, Ritalahti, 2009). Vaikka konstruktiivinen lähestymistapa muistuttaa lähestymistapana innovaatioiden tuottamista, ei se sitä kuitenkaan ole sillä läheskään kaikki konstruktiot eli lopputulemat eivät ole innovaatioita. Konstruktiivinen menetelmä sopi mielestäni tähän opinnäytetyöhön parhaiten, sillä tarkoituksena oli luoda yritykselle tietoturvapolitiikka, jota ei aikaisemmin ollut. Tietoturvapolitiikka on aiheena hyvin tunnettu ja siihen löytyy valmiita malleja ja ohjeita, mutta haasteeksi jää sovittaa tämä tieto vastaamaan kohdeyrityksen tarpeita, sekä resursseja.

Konstruktiviinen tutkimusmenetelmä rakentuu prosessipuusta, joka koostuu kuudesta eri osa-alueesta.Opinnäytetyö on rajattu keskittymään prosessipuun kolmeen ensimmäiseen osaan jossa pyritään ensimmäiseksi selvittämään ongelma, toiseksi tutustua syvälliseen teoreettiseen tietoon sekä kerätä käytännön tietoa tutkimuksesta ja kehittämisen kohteesta, sekä lopulta laatia näiden pohjalta ratkaisut ongelmiin. Prosessipuun muihin osiin ei keskitytä, sillä toimivuuden testaus ja konstruktion oikeellisuuden osoittaminen voi osoittautua liian pitkän aikavälin prosessiksi, kun on kyse opinnäytetyöstä jossa on rajallinen aikataulu. (Ojasalo, Moilanen, Ritalahti, 2009)



Kuvio 1 Konstruktiivisen tutkimuksen prosessipuu ja työn rajaus

2.1 Tiedon perusominaisuudet

Hakalan mukaan, alan kirjallisuus ja erilaiset tietoturvastandardit antavat hieman toisistaan eroavia määritelmiä tietoturvalle, mutta perusajatus on kuitenkin kaikissa sama. Tieto on yrityksen tärkeintä omaisuutta ja tavoitteena on pitää se luotettavana ja vain oikeiden ihmisten saatavilla, oikeassa muodossa, tehokkaasti sekä nopeasti. Klassisen tiedon arvoon perustuvassa määritelmässä Hakala mainitsee tietoturvallisuuden koostuvan kolmesta osatekijästä, tiedon luottamuksellisuudesta, käytettävyydestä, sekä eheydestä. Myöhemmin klassiseen näkökulmaan on lisätty kaksi lisätekijää jotka ovat kiistämättömyys sekä pääsynvalvonta. (Hakala & Vainio & Vuorinen, 2006, s.4-5)

Luottamuksellisuudella tarkoitetaan, että tieto ei päädy sellaiselle henkilöille joilla ei ole okeuksia sen lukemiseen, muokkaamiseen tai tuhoamiseen, vaan tieto pysyy vain siihen oikeutettujen henkilöiden käytettävissä. Käyttäjätunnukset ja salasanat ovat hyvä esimerkki jolla luottamuksellisuus koitetaan turvata. *Käytettävyydellä* tai *saatavuudella* tarkoitetaan sitä, että tieto on käyttäjän saatavilla järjestelmästä riittävän nopeasti ja oikeassa muodossa. Esimerkiksi sähkökatko voi aiheuttaa käyttökatkon jolloin tietojen saatavuus katoaa. Useissa yrityksissä on varavirtalaite suojaamassa tätä skenaariota. Tietojen *eheydellä* tarkoitetaan tiedon paikkaansapitävyyttä ja että se ei sisällä mitään virheitä joka voisi vaarantaa tiedon alkuperäisyyden. (s.4-5)

Kiistämättömyys tarkoittaa, että tietojärjestelmä pystyy tallentamaan tiedot niin, että tiedon alkuperä säilyy, sekä mahdollinen tietojärjestelmien luvaton käyttö. Kiistämättömyyteen pyritään erilaisin keinoin, mm. älykorteilla, biometrisillä tunnistustavoilla kuten sormenjälkitunnistimella tai jollakin muulla usein pienellä mukana kuljetettavalla laitteella josta käyttäjä voidaan todentaa. (Tietojesiturvaksi.fi, accessed 13.5.2014)

Pääsynvalvonnalla pyritään rajaamaan yrityksen tietojenkäsittelyinfrastruktuurin käyttöä jotta se ei ylikuormittuisi ja heikentäisi *käytettävyyttä*. Hakala mainitsee tärkeäksi organisaation estää yrityksen omia työntekijöitä käyttämästä sen laitteita tai tietoliikenneyhteyksiä omiin tarkoituksiinsa. Kohdeyrityksen pienestä koostu johtuen, riski tietoliikenteen ylikuormittumisesta on kuitenkin varsin pieni. (s.5)

3 Tietoturvan johtaminen yrityksessä

Tietoturvallisuus on läsnä nykypäivän yhteiskunnassa ja sen toimivuus on ehdoton edellytys organisaation toiminnalle. Lisäksi yhteiskunta asettaa yrityksille edellytyksiä tietojen turvaamisesta, siten että kansalaisten perusoikeudet tulevat toteutetuksi ja yhteiskunnan toiminnot ja niiden jatkuvuus tulee turvatuksi.(Andreasson & Koivisto, 2013 s.32)

Tietoturvallisuutta tulee toteuttaa organisaatiossa, niin että se tukee yrityksen perustehtäviä ja strategiset tavoitteet tulevat toteutetuksi mahdollisimman kustannustehokkaalla tavalla. Johdon tulee olla keskeisessä roolissa tietoturvallisuuden organisoinnissa, suunnittelussa, ylläpitämisessä ja kehittämisessä. On erityisen tärkeää, että johto sitoutuu sen kehittämiseen. Johdon tulee nimetä vastuuhenkilö ja antaa tälle riittävät resurssit tietoturvavelvoitteiden hoitamiseksi. Raportointia täytyy myös olla molempien osapuolten välillä, jotta ristiriitaisuuksilta vältyttäisiin. Johdon tulee pitää vastuuhenkilö tietoisena mahdollisista hankkeista tai projekteista, jotka saattaisivat vaikuttaa tietoturvallisuuden yleiskuvaan yrityksessä. Vastuuhenkilöiden tulisi myös olla osana päätöksentekoa mahdollisista kehittämistoimista, sekä raportoida johdolle tietoturvallisuuden tilasta, kehityksestä sekä tietoturvavelvoitteiden toteutumisesta. (2013 s.33)

Tietoturvallisuus nähdään osana yrityksen jokapäiväistä toimintaa, jossa yhdistyy tekniikka, lainsäädäntö sekä hallinnolliset toimet. Liiketoiminnan vaatimukset, sekä lainsäädännön määräämät velvoitteet antavat pohjan tietoturvan kokonaisvaltaiseksi kartoittamiseksi. Yleisesti ajatellaan, että tietoturva perustuu pelkästään teknisiin toimiin, mutta (Laaksonen & Co, 2006) painottaa teoksessaan Yrityksen tietoturvakäsikirja, että vasta hallinnollisten toimien kuntoon saattamisen jälkeen voidaan teknisillä ratkaisuilla kehittää ja ylläpitää tietoturvaa. Teknisten toimien käyttöönottamisen jälkeen, tietoturvallisuutta tulee ylläpitää säännöllisellä seurannalla ja kehittämisellä.

Tietoturvapalveluita tarjoava yritys Silverskin teetti vuonna 2012 syksyllä raportin jossa haastateltiin 100 yrityksen ylintä edustajaa tietoturva-asioita koskien. Tietoturvan johtaminen nähtiin useammin teknisten yksityiskohtien huolehtimisena, kuin strategisena kokonaiskuvan hahmottamisena, riskien priorisointina ja tavoitteiden asettamisena. (Silverskin.com, 2014) Todellisuudessa teknisistä yksityiskohdista huolehtiminen on vain pieni osa kokonaisturvallisuutta.

Tyypillisimmät uhkakuvat jotka liittyvät tietoturvan hallinnoimiseen ovat useasti puutteellinen tietoturvan johtaminen, lainsäädännön tai sopimusten rikkomukset, tietoturvasta johtuvien liiketoiminnan häiriöt, tietoturvan puutteellisesta johtamisesta aiheutuva resurssien epätaloudellinen käyttö. (BSI Grundschutz catalogue 2005, B1.0)

BSI kuvaa katalogissaan tapoja joilla uhkia pystytään ennalta ehkäisemään. Jälleen kerran yhdeksi avaintekijäksi muodostuu johdon vankka sitoutuminen tietoturvan tavoitteiden saavuttamiseksi ja ymmärtää oman vastuunsa yrityksen tietoturvan kehittämisessä. Johdon tehtävänä on kontrolloida ja monitoroida hallintaprosessia, niin että se kattaa kaikki yrityksen osastot.

Jotta tietoturvallisuus olisi asianmukaisesti johdettavissa, tulee luoda johdon hyväksymä tietoturvapolitiikka, jonka yksi tavoitte on saada tietoturvallisuus osaksi jokapäiväistä toimintaa.Tietoturvapolitiikka on osa laajempaa tietoturvan johtamista, sillä se on tärkein tietoturvallisuuskäytäntöjä ja tietoturvallisuusprosessia ohjaava dokumentti (Hakala, Vainio Vuorinen, 2006 s.8).

3.1 Tietoturvapolitiikan suhde koko tietoturvan hallintaprosessiin

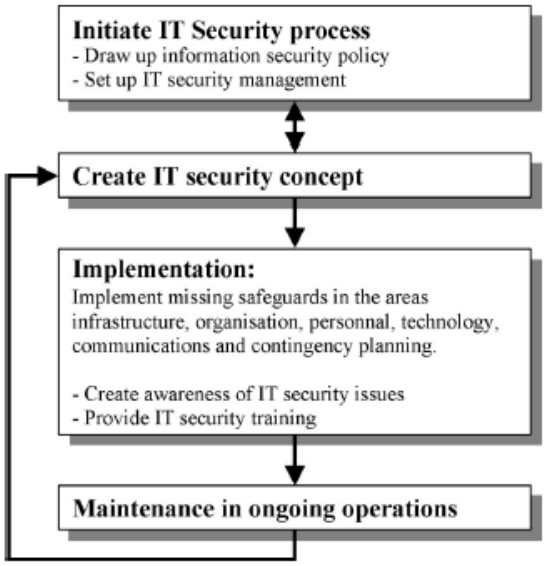
BSI-Grundschutz katalogi (BSI) on saksan valtion tietoturvan kehittämislaitoksen luoma standardeihin perustuva katalogi. Katalogi kuvaa tietoturvan johtamista jatkuvasti käynnissä olevaksi prosessiksi, jossa pyrkimyksenä on nostattaa yrityksen tietoturvan tasoa. Tämä tietoturvan hallintaprosessi on osa tietoturvan strategista täytäntöönpanoa joka pitää sovittaa yrityksen tarpeita vastaavaksi. (BSI-1.0 s.50).Tietoturvaprosessin ensimmäinen vaihe on valmistella tietoturvapolitiikka joka on osa laajempaa tietoturvan johtamista. Tietoturvapolitiikan merkitystä ja sisältöä käsitellään tarkemmin seuraavassa luvussa.

Tietoturvapolitiikan merkityksen ymmärtämiseksi on tiedostettava, tietoturvapolitiikka luo puitteet jatkotoimenpiteille joihin kuuluu se, että tietoturvalle tulee luoda viitekehys/runko, johon vaikuttaa yrityksen koko, tarpeet ja resurssit. Johdon tulee nimetä tietoturvasta vastaavat henkilöt, sekä määrittää heidän vastuunsa, tehtävänsä ja valtuudet. Samoin tulee kuvata yrityksen kaikki järjestelmät ja mitä tietoa niissä liikkuu jotta tietoturva konseptin suunnittelussa tulisi jäsenneltyä kaikki mahdolliset haavoittuvuudet. (BSI – S2.195)

Implementointivaiheessa asetetaan kaikki tietoturvatoimenpiteet käytäntöön. (BSI – S2.191, s.1254)

Jotta yrityksen tietoturvallisuusdesta tulisi kattava, tulee henkilökunnan toimia aktiivisessa roolissa uhkien havaitsemiseksi. Henkilökunnalle tulee antaa asianmukaista koulutusta tätä varten jotta raportointi toimisi tehokkaasti. (BSI - S2.191, s1254.)

Kun implementointivaihe on saatu päätökseen, prosessi jatkuu ylläpitovaiheessa. Saavuttaakseen pitkäaikaisen suojan tietoturvan ylläpitoon, yrityksen tulee jatkuvasti tarkastella mahdollisia liiketoiminnallisia muutoksia, tietoturvaonnettomuuksia, teknisiä muutoksia tai muita uhkakuvia jotka saattavat suhteessa vaikuttaa tietoturvallisuuden tasoon. (BSI - S2.191, s.1254)



Kuvio 2 Tietoturvan hallintaprosessi BSI:n mukaan

3.2 Tietoturvapolitiikka

Tietoturvapolitiikka on yrityksen johdon hyväksymä dokumentti jossa yrityksen strategiset tavoitteet ohjaavat tietoturvallisuuden systemaattista kehittämistä. Laaksonen, Nevasalo ja Tomula (2006, s.146) kuvailee politiikkaa luonteeltaan pysyväksi tahtotilaksi jota voidaan päivittää tarvittaessa.

Politiikassa määritellään yrityksen käytänteet, eli menetelmäkokonaisuudet jokaisessa eri liiketoimintaprosessissa tai tietojärjestelmässä. (2006 s.7) Menetelmien tulee myös noudattaa tiedon arvoon perustuvia määritelmiä; *tiedon luottamuksellisuus, käytettävyys ja eheys.* (SOGP, 2007)

Tietoturvapolitiikka on siis eräänlainen johdon asettama strateginen linjaus joka toimii ohjeena tietoturvaa suunnitteleville henkilöille tai liiketoimintaprosesseista vastaaville esimiehille. Vaikka politiikan tarkoituksena on toimia n.5-10 vuoden aikavälin ohjeena, tulisi sitä tarkastella vähintään vuoden välein ja katsoa vastaako se yrityksen nykytilaa ja tarpeita (Laaksonen & co.2006 s.7).

Alan kirjallisuudesta ja internetistä löytyy paljon esimerkkejä tietoturvapolitiikoista, mutta se mikä toimii yhdelle ei välttämättä sovellu toisen yrityksen tarpeisiin, sillä tietoturvapolitiikka kertoo mikä on tietoturvan merkitys yritykselle.(Vahti 3/2007)

Ennen tietoturvapolitiikan luomista yrityksen tulee luoda ja taltioida omat tietoturva-tavoitteensa, sillä ne luovat pohjan tietoturvapolitiikan luomiselle. (BSI-S.2.192, s.1256) Tietoturvapolitiikka kertoo johdon näkemyksen, miten tietoturvallisuus vaikuttaa organisaation toimintaan ja miten yrityksessä siihen pitäisi suhtautua. (Laaksonen & co. s.147)Tavoitteiden luomiseksi pitää tarkastella yrityksen liiketoimintaprosesseja sekä niihin liittyviä teknisiä tehtäviä. Myös lainsäädäntö ja yrityksen yleiset päämäärät antavat pohjaa tavoitteiden synnylle ja lopulta politiikan luomiselle. (BSI-S.2.192, s.1256)

Tietoturvapolitiikka pitäisi kirjoittaa aina sellaseen muotoon, että muutkin kuin tietotekniikan ammattilaset osaisivat tulkita sitä. (Hakala & Co, s.9) Tietoturvapolitiikka on usein julkinen dokumentti, koska sillä pystytään osoittamaan yhteistyökumppaneile ja asiakkaille mikä tietoturvan asema on yrityksessä ja mitä se merkitsee kuinka heille. Tietoturvapolitiikan pohjalta tehdään myös käytännön tietoturvaohjeet työntekijöille. Nämä yksityiskohtaisemmat ohjeet ovat luonteeltaan salaisia tai luottamuksellisia. Ohjeet kuvaavat tarkemmin jotkin käytänteet tai tekniset menetelmät tietojen suojaamiselle. (Hakala & Co, s.9)

Suuremmissa yrityksissä ja organisaatioissa tietoturvaohjeistus voidaan jakaa eri organisaation osia koskeviin ohjeisiin, kuten yleisiin ohjeisiin tai jotakin tiettyä osa-aluetta koskeviin erityisohjeisiin. (Andreasson & Koivisto, 2013, s.44) Esimerkki tälläisistä ohjeista tarjoaa, Suomen valtiovarainministeriön tietoturvaohjeet, jotka ovat hyvin monipuoliset ja kattavat eri tietoturvan osa-alueita. Valtiovarainministeriön ohjeet ovat julkista tietoa ja niihin voi tutustua heidän web-sivuillaan..

Tietoturvapolitiikan sisältö vaihtelee yrityksittäin, mutta hyvä tietoturvapolitiikka sisältää yrityksen tietoturvatavoitteet, kohteet ja periaatteet, sekä vastuiden määrittelyn. Myös lainsäädännön tuomat velvoitteet ja sopimusten tuomat vaatimukset tulee sisällyttää tietoturvapolitiikkan.

BSI-Katalogin mukaan tietoturvapolitiikan pitää olla selkeä ja helposti ymmärrettävä ja vähimmäisvaatimuksena sen pitää täyttää tietyt ehdot. Politiikan pitää osoittaa tietoturvan tärkeys ja tietotekniikan merkityksen yritykselle, sekä havainnollistaa tietoturva tavoitteiden tärkeys suhteessa liiketoimintatavoitteisiin. Politiikan tulisi sisällyttää tietoturvastrategian avaintekijät ja sen tulisi kertoa henkilöstölle, että johto on tietoturvapolitiikasta ja sen onnistumisesta vastuussa. Sen tulisi myös sisällyttää minkälainen on yrityksen organisaatiorakenne suhteessa tietoturvallisuuteen. (BSI-S2.192, s.1257)

Jotta tietoturvapolitiikasta saisi kaiken hyödyn irti, tulisi tietoturvallisuuskoulutus sisällyttää osaksi politiikkaa. Politiikassa tulisi määritellä tietoturvallisuuskoulutuksen vaatimukset, jotta henkilöstö ymmärtäisi ja sisäistäisi tietoturvapolitiikan tavoitteet ja toimenpiteet, joilla nämä tavoitteet saavutetaan. (Laaksonen & Co. s147) Myös yleiset linjaukset kuten maininta liiketoiminnan jatkuvuus- ja toipumissuunnitelmista kuuluvat politiikkaan.

Tietoturvapolitiikkaan tulisi sisällyttää myös mahdolliset seuraamukset tietoturvapolitiikan laiminlyönnistä. Tietoturvaohjeiden tulisi tuoda esille, mikä on sallittua ja mikä ei, sekä tiedottaa ohjeiden laiminlyönnistä aiheutuvat sanktiot.

BSI-Katalogin mukaan, työntekijät jotka ymmärtävät joidenkin tietoturvaprosessien perimmäisen merkityksen noudattavat ohjeita tehokkaammin. (BSI-S2.192, s1257) Jotta näin olisi, tulee tietoturvapolitiikan olla sellaisessa muodossa joka ajaa yrityksen perimmäisiä strategisia tavoitteita. Kaikki uudet työntekijät tulee perehdyttää tietoturvapolitiikkaan ja tietoturvaohjeisiin, ennen kuin he alkavat käyttää yrityksen tietojärjestelmiä. Usein työsuhteen alkaessa, työntekijät joutuvat allekirjoittamaan ymmärtävänsä politiikan sisällön.

3.3 Tietoturvasuunnitelma

Tietoturvapolitiikka asettaa puitteet yrityksen tai organisaation tietoturvasuunnitelmalle. Poiketen tietoturvapolitiikasta, tietoturvasuunnitelma pyritään laatimaan usein keskipitkälle aikavälille n.2-5 vuotta. Tämä johtuu siitä, että toisin kuin tietoturvapolitiikassa, tietoturvasuunnitelmassa käytänteet ovat paljon konkreettisemmassa muodossa. Työmenetelmät ja tekniset ratkaisut kuhunkin tietotojärjestelmään pyritään kirjaamaan paljon yksityiskohtaisemmin. Tekniikan kehittyessä vuosi vuodelta, joutuu myös tietoturvasuunnitelmaakin katsastaa vuosittain, sillä aina kun tietojärjestelmää muokataan tai päivitetään, tulee myös työmenetelmiin muutoksia ja nämä muutokset täytyy päivittää suunnitelmaan vastaaviksi.

Tietoturvasuunnitelman laatimisesta vastaavat usein tietoturvapäällikkö yhdessä tietohallinnon ja tietojenkäsittelyn ammattilaisten kanssa. Tietoturvasuunnitelma on luonteeltaan luottamuksellista tai salaista tietoa. (Hakala & Vainio & Vuorinen)

3.4 Lainsäädännön asettamat vaatimukset tietoturvalle

Suomessa ei ole erikseen säädettyä tietoturvalakia, mutta yrityksillä on silti lainsäädännöllisiä velvoitteita tietoturvaansa liittyen. Näistä velvoitteista on säädetty Suomen yleislaeissa. Yritykset jotka keräävät, tallettavat tai muutoin käsittelevät työntekijöidensä tai asiakkaitensa henkilötietoja tulee noudattaa suomen henkilötietolakia (22.4.1999/523), sekä muita siihen liittyviä yleisvelvoitteita.

Henkilötietolain tarkoituksena on suojata ihmisten yksityisyydensuoja ja parantaa hyvän tietojenkäsittelyn tapaa. (Tietosuojavaltuutetun toimisto, 2014)*”Henkilötiedolla tarkoitetaan kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi*.” (Henkilötietolaki 22.4.1999/523 §3)

Useat yritykset keräävät asiakkaiden tai henkilöstön henkilötietoja omiin tarkoituksiinsa, usein tiedot tallennetaan sellaiseen muotoon jota voidaan kutsua henkilörekisteriksi. *”Henkilörekisterillä tarkoitetaan sellaista henkilötietoja sisältävää tietojoukkoa jota käistellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta*.” (Henkilötietolaki 22.4.1999/523 §3)

Henkilörekisterin pitäjälle täytyy nimetä vastuuhenkilö, joka on vastuussa siitä, että henkilötietoja käsiteltäessä käytetään hyvää tietojenkäsittely tapaa. Hyvän tietojenkäsittelytavan tärkeimpiin periaatteisiin kuuluu huolellisuus-, suunnittelu-, tarpeellisuus ja suojaamisvelvoitteet. Vastuuhenkilön täytyy myös pitää huoli siitä, että rekisteriseloste on yleisesti saatavilla, useasti yrityksen web-sivuilta. Rekisterinpitäjällä on myös virheettömyysvaatimus, joka merkitsee sitä että se ei käsittele virheellisiä tai vanhentuneita henkilötietoja. (Finlex, 2014)

Toinen tietoturvallisuuteen liittyvä laki on ”Sähköisen viestinnän tietosuojalaki” jonka merkitys muille kuin teleliikennepalveluja tarjoaville yrityksille koskee lähinnä työnantajan oikeuksia avata yrityksen työntekijälleen luovuttaman sähköpostin viestejä.

3.5 Ulkoistaminen, sekä sopimukset

Ulkoistaminen näkyy yritysten liiketoimintastrategioissa jo selvästi ja tämä trendi tulee kasvamaan myös tulevaisuudessa. Osasyy miksi ulkoistaminen kiinnostaa yrityksiä johtuu siitä, että ulkoistamisen jälkeen yritys pystyy keskittymään paremmin omien ydintoimintojensa parantamiseen. Myös kustannustehokkuus houkuttelee entistä enemmän yrityksiä ulkoistamaan osaa liiketoimintaansa, sillä tämän ulkoistetun osan IT-laitteiden ylläpito ja hallinnoiminen ei tuota kustannuksia, vaan sisältyy ulkoistetun palvelun hintaan. Ulkoistettu

palvelu tarjoaa myös usein mahdollisuuksia saada asiantuntija-apua tältä tietyltä osa-alueelta. (BSI-Grundschutz, B1.11 Outsourcing, 2013)

Palvelun ulkoistaminen ulkopuolisen toimijan hoidettavaksi ei esimerkiksi vapauta yritystä rekisterinpitäjän lakisääteisistä velvollisuuksista.

Pilvipalveluilla (*cloud computing)* tarkoitetaan sellaisia tietotekniikkaratkaisuja, joissa käyttöön otetaan palveluntarjoajan tuoma ohjelmisto, levykapasiteetti tai laskentatehoa edistävä palvelu joka toimii internetin välityksellä palveluntarjoajan tiloissa. Yritykseltä siirtyy siis tieto oman verkon ja hallinnan ulkopuolelle. Tämä voi aiheuttaa myös huolia yritykselle tietoturvallisuuden osalta, jos kaikkia riskejä ei ole otettu huomioon viimeistään sopimuksentekovaiheessa. Jos yritys aikoo ottaa käyttöön pilvipalveun, yrityksen tulisi selvittää palveluntarjoajalta missä tiedot sijaitsevat ja kuinka niitä suojataan, sekä selvittää kuka tietoja käsittelee ja kuinka niiden käyttöä valvotaan. Yrityksen tulisi selvittää vastaako palvelun tietoturva asiakkaan tarpeita, sekä selvittää onko palveluntarjoajan ns. standardisopimuksessa otettu huomioon tietoturva-asiat, sekä vastuut. (Andreasson & Koivisto, 2013 s.26)

Mahdollisten sanktioiden määritteleminen voi olla hyvinkin vaikeaa, jos ulkoistamis-sopimuksissa ei ole määritelty tarkkaan vastuunjakoa. Riittämätön vastuiden ja roolien määrittely onkin yksi yleisimmistä tieoturvallisuuteen liittyvistä ongelmista ulkoistamistilanteissa. Paras tapa varautua ulkoistamistilanteeseen on laatia sopimuksiin tarkka vastuunjako. (Laaksonen, 2006, s.239)

Laatiessa ulkoistamissopimusta ulkoistamispalveluntarjoajan kanssa tulisi ulkoistajan, eli yrityksen joka hankkii palvelua, ottaa lainsäädännölliset velvoitteet huomioon. Henkilötietolaki velvoittaa yritystä tekemään kirjallisen sopimuksen, mikäli yritys siirtää oman henkilörekisterinsä jonkin toisen yrityksen ylläpidettäväksi. Näiden velvoitteiden hoitamiseksi tulisi määrittää vastuu tietoturvan osalta molempien osapuolten välille. (Henkilötietolaki 32 §)

4 Yrityksen tietoturvallisuuden nykytason analyysi

Koska kohdeyhtiön tietoturvasta ei ollut kokonaisvaltaista käsitystä päätettiin suorittaa tietoturvallisuuden nykytilan analyysi, joka toimisi perustana tietoturvapolitiikan laatimiselle ja pohjaksi keskusteluille yrityksen johdon kanssa.

Tiedot kerättiin haastattelemalla yrityksen työntekijöitä, toimitusjohtajaa, sekä tietohallintovastaavaa. Työntekijöiden haastattelussa, haastattelumenetelmänä käytettiin avointa haastattelua, missä haastattelija ja haastateltava keskustelivat avoimesti työntekijän työprosesseista, sekä niihin liittyvistä tietoteknisistä asioista. Tyypillistä avoimessa haastattelumenetelmässä on se, että keskustelu on avointa ja epämuodollista. (Ojasalo, Moilanen, Ritalahti, 2009, s.97) Samaa tekniikkaa käytettiin myös kun haastateltiin yrityksen

toimitusjohtajaa ja tietohallintovastaavaa. Kerättyjen tietojen perusteella, tehtiin yhdessä tietoturvavastaavan kanssa tietoturva-analyysi.

Yrityksen tietoturvan analysointi voidaan tehdä eri tavoin, mutta tässä arvioinnissa on käytetty apuna valtiovarainministeriön ohjetta (VAHTI 2/2010). Siinä tietoturvan arviointi jaetaan kahteen eri osaan jossa ensimmäisenä tarkastellaan organisaation tietoturvallisuutta, sen hallintaa ja organisointia ja toisessa osassa arvioidaan IT-prosessien nykytasoa.

Tarkastelu tehtiin, jotta nähtäisiin missä osa-alueissa yrityksellä on puutteita ja mitkä kohdat ovat jo huomioitu tarpeeksi hyvin. Käytetty analyysimenetelmä tuottaa tulosteeksi graafisen esityksen mistä on helppo nähdä kokonaistilanne ja tehdä johtopäätöksiä.

4.1 Organisaation hallinnollinen tietoturvallisuus

Organisaation tietoturvallisuuden hallinta jaetaan johtajuuteen, strategisen toiminnan suunnittelun, henkilöstöön liittyviin seikkoihin, kumppanuuksien ja resurssien ylläpitämiseen sekä prosesseihin ja mittaamiseen.

Analyysi tehtiin haastattelemalla yrityksen tietoturva-asioista vastaavaa hallintojohtajaa. Tiedot syötettiin excel pohjaiseen taulukkoon, jossa toteutuva taso perustuu numero-arvoon. Organisaation tietoturvallisuuden hallinnan kaaviossa vaaleanpunainen viiva näyttää tavoitetason ja tummempi punainen alue näyttää nykytason. Tasot jakautuvat lakisääteisiin vaatimuksiin, perustason vaatimuksiin, korotettujen tasojen vaatimuksiin- ja korkean tason vaatimuksiin. Lähtökohtaisesti tavoitetasoiksi asetetiin, että kaikki lakisääteiset vaatimukset ja osa perustason vaatimuksista täytetään ja tapauskohtaisesti katsotaan korotetun ja korkean tason vaatimukset, jos nähdään että niistä saattaisi olla kilpailuetua yrityksen liiketoimintastrategiassa.

Tuloksia tarkasteltiin yhdessä yrityksen johdon kanssa osa-alueittain.

Kuvio 3 VAHTI hallinnallisen tietoturvan nykytila-analyysi

4.1.1 Johtaminen

Yrityksen strategisessa ohjauksessa huomattiin puitteita, sillä vain yksi perustason vaatimuksista täyttyi. Organisaation ydintoiminnot ja prosessit ovat tunnistettu ja vastuutettu. Yritys ei kuitenkaan ole tiedottanut ja vastuuttanut henkilöstöä lain asettamista vaatimuksista toimintaansa koskien, eikä yrityksellä ole kirjallista johdon hyväksymää tietoturvapolitiikkaa. Yrityksellä ei ollut strategiatason suunnitelmaa kirjallisena, mistä käy ilmi miten tietoturva vastuutetaan ja organisoidaan ydintavoitteiden saavuttamiseksi. Tietoturvallisuuden vuosittainen kehittämissuunnitelma puuttui myös.

Yrityksen resursoinnissa ja organisoinnissa yritys toimii yli odotetun vaatimustason ja täyttää kaikki perustason ja korotetun tason vaatimukset. Selityksenä on se, että pienessä organisaatiossa tietoturvan hallintaresursseihin kuuluu vain yksi henkilö, tietoturvavastaava jolla on aikaa vastuidensa hoitamiseen. Yrityksellä on siten kokoonsa nähden riittävästi tietoturvahenkilöstöä ja resursointi on otettu huomioon yrityksen budjetoinnissa sekä talous- ja toimintasuunnitelmissa.

Johto ei ole organisoinut tai vastuuttanut tiedottamista asiakkaita koskevista tietoturva asioista. Tässä nähtiin parantamisen varaa, sillä muun muassa rekisteriseloste puuttui sidosryhmien saatavilta.

Erityistilanteiden johtamisessa nähtiin parantamisen varaa. Perustason vaatimuksiin kuuluu, että tietoturvapoikkeamien käsittely olisi organisoitu ja vastuutettu. Myöskään vakavista tietoturvapoikkeamista ei pidetä kirjaa mikä saattaa aiheuttaa sen, että tietoturvauhka jää hoitamatta. Myös johdon raportoinnissa mikään perustason vaatimuksista ei täyttynyt. Perustason vaatimuksiin kuuluu, että tietoturvallisuudesta raportointi olisi vastuutettu ja organisoitu, sekä tietoturva-asioista raportoitaisiin säännöllisin väliajoin yrityksen johdolle ja tietoturvavastaavalle puolin ja toisin. Tätä ei yrityksen ja johtoryhmän koko huomioonottaen nähty kuitenkaan oleellisena puutteena.

Tällä hetkellä osa johtajuuteen liittyvissä vaatimuksissa yritys toimii yli odotusten, mutta raportoinnissa yrityksen sisällä, tietoa ei välttämättä dokumentoida. Yrityksen ulkopuolisille sidosryhmille ei myöskään raportoida tietoturvaan liittyviä asioita.

4.1.2 Strategiat ja toiminnan suunnittelu

Erityistilanteiden hallinnassa Yritys täyttää kaikki perus-, -korotetun-, ja korkean tason vaatimukset. Yrityksellä ei ole mitään yhteiskunnan elintärkeiden toimintojen turvaamiseen liittyviä vastuita joten ne eivät ole oleellisia. Yrityksellä on myös jatkuvuussuunnitelma tärkeiden tietojen varastoimiseen liittyen. Jatkuvuussuunnitelmaa myös, testataan ja toimivuutta harjoitellaan säännöllisesti.

Toimintaympäristön vaikutuksessa vain yksi perustason vaatimuksista täyttyi. Erilliset tietojenkäsittelyn toimintaympäristöt ja niihin kuuluvat järjestelmät ja toiminnot ovat tunnistettu, mutta näiden toimintaympäristöjen erityisvaatimukset ja tavoitteet eivät.

Tavoitteiden määrittelyssä mikään perustason vaatimuksista ei täyttynyt. Perustason vaatimuksiin lukeutuu se että kunkin ydintoimintojen kannalta tärkeimmät suojattavat kohteet ovat tunnistettu ja luokiteltu vaadittavan tietoturvan tason mukaisesti.

Toiminnan kehittäminen riskien arvioinnilla kaikki perustason vaatimukset täyttyivät, sillä yrityksessä tehdään säännöllisesti tietoturvaa koskevaa riskien arviointia, sekä riskien perusteella parannetaan tietoturvaa, kaikkea ei silti välttämättä dokumentoida.

Toimintaverkoston hallinnassa kaikki perustason vaatimukset täyttyivät. Yritys on tietoinen missä toimintaverkostoissa se on mukana ja mitä alihankkijoita ja yhteistyökumppaneita sen tietojen kanssa toimii missäkin roolissa.

4.1.3 Henkilöstö

Henkilöstön osaamisen ja tietoisuuden kehittämisessä ja sanktioinnissa ilmeni paljon puutteita, sillä mikään perustason vaatimuksista ei täyttynyt. Yritys ei pidä henkilöstölle

tietoturvakoulutuksia, eikä työntekijän perehdyttämistilanteessa käydä läpi tarvittavia tietoturvaan liittyviä asioita. Muuttuneista tietoturvakäytänteistä ei myöskään tiedoteta tarpeeksi hyvin henkilöstölle.

Henkilöresurssien ja tehtävien hallinnassa perustason vaatimukset täyttyivät, sillä yrityksen valitut tietoturvatoimenpiteet- ja prosessit ovat vastuutettu ja organisoitu. Myös avainroolit kuka on vastuussa tietoturvasta on nimetty ja vastuutettu tehtäviinsä.

Yritys toimii erityistilanteissa hyvin, sillä yritys huolehtii sähköisen viestinnän tietosuojalaista 4§ ja 5§, sekä laista yksityisyyden suojasta työelämässä 6.luku. Näihin lukeutuu sähköisten viestien, kuten sähköpostien paikkatietojen sekä tunnistamistietojen huolellinen käsittely. Henkilöstö on tietoinen kenelle tietoturvapoikkeamista kuuluu ilmoittaa ja tietoturvapoikkeamien vastuuhenkilö on koulutettu tehtäväänsä.

4.1.4 Kumppanuudet ja resurssien hallinta

Sopimusten hallinnassa yritys toimi tietoturvaan nähden huonosti, sillä vain yksi perustason vaatimuksista täyttyi. Kumppanuus- ja hankintatoiminta on vastuutettu ja organisoitu, mutta yhteistyökumppanien kanssa ei oltu tehty asianmukaisia sopimuksia. Perustason vaatimukseen kuuluisi, että tehdään kirjallinen sopimus, jossa määritellään mahdolliset tietoturvavaatimukset sekä miten näiden vaatimusten raportointi, auditointi ja seuranta tapahtuu. Kumppanuuksien välinen yhteistyö ei toimi erityistilanteissa kovinkaan hyvin, sillä kumpaakaan osapuolta ei sido mikään ilmoittamaan tai raportoimaan tietoturvapoikkeamista toiselle. Kirjallisen sopimuksen puute, tietoturvavaatimuksineen oli suurin ongelma tässä aihealueessa.

Yrityksellä on käytössään toiminnanohjausjärjestelmä johon kirjataan luottamuksellisia tietoja kuten asiakasrekistereitä, kauppakirjoja ja toimeksiantoja. Tämä ulkoistettu palvelu toimii yhtenä ydinliiketoimintaprosessina ja koska palvelua käyttämällä tallennetaan tietoa palveluntarjoajan pilveen, tulee myös tarkastella miten palveluntarjoaja on ottanut huomioon tietoturvan tason.

Palvelun vanha versio otettiin käyttöön vuonna 2000, eivätkä osapuolet tehneet kirjallista sopimusta palvelun käyttöönotosta. Uusi versio otettiin käyttöön myöhemmin vuonna 2010. Vaikka yritys ei itse vastaaa toiminnanohjausjärjestelmän tietoturvasta, tulisi asia kuitenkin hoitaa samalla tavalla kuin mikä tahansa muukin yrityksen toiminto. Ulkoistamistilanteessa on erityisen tärkeää saada esille sopimuksiin osapuolten vastuunjako, sillä virhe ja rikkomustilanteissa tietoturvallisuuden osalta, vastuuasemassa on usein ulkoistuksen tehnyt yritys, eikä palveluntarjoaja. (Henkilötietolaki 32 §)

4.1.5 Liiketoiminnan prosessit

Tietoaineistojen hallinnassa yritys toimii erittäin hyvin. Yrityksen työntekijät ovat tietoisia miten tietoaineistoa käsitellään yrityksessä ja miten luottamukselliset asiakirjat hävitetään

eri liiketoimintaprosesseissa, niin että kohteen tietosuoja varmistetaan. Yritykseltä löytyy myös kirjallinen ohje siitä, miten asiakirjat hyväksytään ja katselmoidaan ja mikä yrityksen tiedoista ovat salassapidettävää tai vaitiolovelvollisuuden alaista.

4.1.6 Toiminnan oma-arviointi

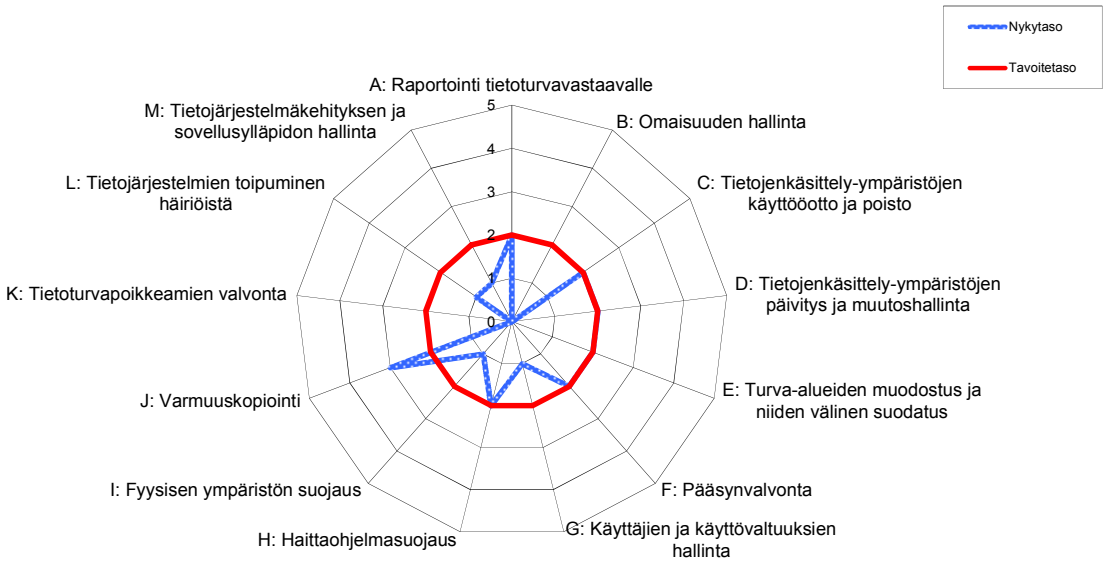
Mikään vaatimuksista ei täyttynyt. Yrityksellä ei ole käytössään säännöllisiä tietoturva auditointeja tai arviointeja.

4.2 Nykytilan analyysi IT-prosessien näkökulmasta

Tässä osassa arvioidaan IT-prosessien nykytasoa ja siinä keskitytään enemmän teknisiin seikkoihin kuten varmuuskopiointiin, tietojenkäsittelyn ympäristöihin, käyttövaltuuksien hallintaan, pääsynvalvontaan ym.

IT-prosessien arviointikaaviossa, sininen viiva näyttää nykytason arvon ja punainen näyttää tavoitetason.

Raportointi toimii perusvaatimusten mukaisesti yrityksessä, sillä henkilöstö raportoi mahdollisista IT-järjestelmien muutoksista tietoturvasta vastaavalle henkilölle. Raportointi toimii puolin ja toisin, jos muutoksia tulee järjestelmiin, henkilöstö saa usein tiedon siitä sähköpostitse tai kasvotusten.



Kuvio 4 VAHTI it-prosessien tietoturvan nykytila-analyysi

Tietojärjestelmien ja työasemien käyttöönotossa ja poistossa huomioidaan järjestelmän tietosisällön tietoturvavaatimukset. Myös käyttöönottoon ja poistamiseen liittyvät toimet ovat organisoitu ja vastuutettu tietoturvasta vastaavalle henkilölle. Tietojärjestelmien päivitys ja huollot ovat myös vastuutettu ja organisoitu hyvin.

Yritys on tunnistanut tietoverkon eri suojaustasoa vaativat osat ja eri suojaustasojen välistä liikennettä suodatetaan sekä rajoitetaan. Palomuurisääntöjen suodatusasetukset ja rajoitukset ovat vastuutettu tietoturvasta vastaavalle henkilölle, mutta niitä ei ole dokumentoitu. Yrityksellä on kirjalliset etäkäyttöyhteys periaatteet, jossa kerrotaan minkälaisita laitteista ja mistä eri verkoista yhteyden voi muodostaa.

Yrityksellä on käytössä useita ulkoistettuja tai ulkoisten palveluntarjoajien tuottamia palveluita joiden käyttö edellyttää henkilökohtaista salasanaa.

Yritys täyttää kaikki perusvaatimusten kriteerit pääsynvalvonnan kannalta. Huonolaatuisten sanasalojen käyttöä estetään. Onnistuneet- ja epäonnistuneet kirjautumisyritykset tallennetaan lokiin, josta käyttäjä voidaan tunnistaa ja yhdistää hänen henkilöllisyyteensä. Tietojärjestelmien omistaja hyväksyy kuinka vahvaa tunnistautumista järjestelmään tarvitaan. Yrityksessä käytetään henkilökohtaisia tunnuksia joiden käyttöä hallinnoidaan ja organisoidaan. Käyttöoikeudet perustuvat työsopimukseen, jonka päätyttyä käyttö estetään teknisin menetelmin viivytyksettä.

Haittaohjelmasuojausta käytetään työasematasolla, sekä niitä päivitetään säännöllisin väliajoin. Käyttäjiä ei ole ohjeistettu miten haittaohjelmia levittäviä sähköposteja voidaan yrittää tunnistaa. Fyysinen suojaus on otettu tarpeeksi hyvin huomioon, yrityksellä on vain pieni määrä omaa laitteistoa jonne pääsyä valvotaan jatkuvasti.

Varmuuskopionti on yrityksessä hoidettu varsin mallikkaasti, sillä varmuskopioinnista on tehty kirjalliset ohjeet. Kaikki suojattavat kohteet ja tallennettavat tiedot ovat tunnistettu ja organisointi on vastuutettu tietylle henkilölle. Tärkeimmistä tiedoista otetaan myös suojakopioita joita säilytetään eri paikassa kuin varsinaisia varmuuskopioita.

Yrityksen tietoturvasta vastaava henkilö tietää omat vastuunsa ja vastaava on kirjoitanut tärkeimmistä järjestelmistä toipumissuunnitelmat.

5 Tietoturvapolitiikan laatiminen pieyrityksessä

Nykytilan analysoinnin jälkeen tietoturvapolitiikan laatiminen aloitettiin yritysjohdon kanssa projektiluontoisesti. Tietoturvapolitiikan laatimista edeltävät toimenpiteet käytiin läpi yhteisissä kokouksissa. Niissä kirjattiin muistiin tietoturvapolitiikan kannalta keskeiset asiat varsinaisen julkaistavaksi tarkoitetun tietoturvapolitiikka-asiakirjan pohjaksi.

5.1 Yrityksen strategia ja tavoitteet

Kohdeyrityksen liiketoimintastrategian keskeiset elementit ovat:

- tuottaa laadukkaita, luotettavia ja yksilöllisiä palveluita asiakkailleen
- tavoittella tyytyväisiä asiakkaita ja pitkäkestoisia asiakassuhteita.
- ei kilpailla halvalla hinnalla vaan pyritään löytämään ne asiakkaat jotka ovat valmiita maksamaan laadusta ja turvallisuudesta.

Strategiset tavoitteet asettavat yritykselle suuret vaatimukset turvata asiakkaittensa luottamuksellisten tietojen turvallisuus. Koska liiketoimintaprosesseissa käsitellään asiakkaiden taloudellisia- ja elämäntilanteeseen liittyviä tietoja, pankkitilitietoja ja henkilötunnuksia on tärkeää, että tiedot eivät pääse vuotamaan yrityksen järjestelmistä, muutu tai katoa. Tietoturvallisuuspuutteista johtuva maineen menetys voisi olla yrityksen liiketoiminnalle kohtalokasta.

Tärkeimpien tietojen eheys, käytettävyys, sekä saatavuus ovat yritykselle kriittisiä yrityksen jatkuvuuden, sekä mahdollisen maineen menetyksen kannalta.

5.2 Tietoturvatavoitteet

Tärkeimmät tietoturvatavoitteet määriteltiin tarkastelemalla yrityksen liiketoimintaprosesseja, resursseja sekä alan lainsäädäntöä.

Asuntokaupassa on asunnon tai kiinteistön ostajalla mahdollisuus tehdä reklamaatioita tekemänäänsä kauppaan liittyen, asuntokaupassa 2 vuoden ja kiinteistön kaupassa 5 vuoden ajan kaupantekohetkestä. Välitysliike on vastuussa siitä, että se on antanut kaiken sen oleellisen tiedon myytävästä kohteesta jolla on voinut olla merkitystä ostajalle kauppaa päätettäessä. Jos myöhemmin syntyy riitatilanne, niin välitysliikkeellä täytyy olla tallessa kaikki se tieto mitä käyttäen se pystyy osoittamaan toimineensa huolellisesti ja oikein. Tästä syystä, tiedot tulee tallentaa turvallisesti ja pitkäkestoisesti siten, että tiedon eheys, käytettävyys tai -saatavuus eivät vaarannu. Suurin osa tiedoista kulkee sähköpostin välityksellä ja tallentuu sähköpostipalvelimelle ja yrityksen omaan tietojärjestelmään. Jos yrityksen työntekijä poistuu yrityksen palveluksesta, niin yrityksellä tulee olla oikeus päästä käsiksi myös näihin tietoihin.

Tietotekniikalla on keskeinen rooli nykyaikaisen kiinteistönvälitysliikkeen toiminnassa. Kiinteistönvälitysliikkeillä on lakisääteinen velvollisuus ylläpitää ajantasaista rekisteriä myynti- ja ostotoimeksiannoista. Tämä rekisteri on kohdeyrityksessä sähköinen tietokanta ja siihen on yhdistetty välitysprosessin muitakin osia, mm. markkinoinnin työkaluja jotka automaattisesti päivittävät asuntomarkkinoinnissa käytettyjä markkinointiportaaleja. Tavoitteena tulee olla, että liiketoimintaprosessin kannalta kriittiset tietojärjestelmät toimivat keskeytyksettä ja ovat häiriötilanteessa palautettavissa mahdollisimman nopeasti.

Osana välitysprosessia laaditaan asuntoja ja kiinteistöjä koskevia kauppakirjoja joiden lopullisissa versioissa esiintyy osapuolten tunnistetietoja kuten henkilötunnuksia. Näitä asiakirjoja joudutaan prosessin kuluessa vaihtamaan mm. sähköpostilla. Tavoitteena tulee olla se, että näiltä osin noudatetaan asiaan liittyvää lainsäädäntöä.

Edellisten lisäksi potentiaalisista asuntojen ostajien henkilötietoja kerätään ja talletetaan myöhempia yhteydenottoja varten. Nämä tiedot muodostavat sähköisen rekisterin jonka sisällöstä tulisi olla rekisteriseloste annettavaksi tietojen luovuttajille.

Yrityksen henkilöstö- ja taloudelliset resurssit asettavat rajoituksia tietoturvallisuuden hallinnoinnin ja järjestelmien toteuttamiselle mikä tule ottaa huomioon.

Koska jatkuvasti otetaan käyttöön uusia palveluja tai laitteita tulee tietoturvavaatimukset ottaa myös käyttöönoton suunnittelussa huomioon.

5.3 Ulkoistamisen asettamat vaatimukset

Yritys käyttää ulkoisia palveluntarjoajia kiinteistönvälitysprosessin ja sähköpostipalveluiden osalta. Vastuu lakisääteisistä velvollisuuksista säilyy kuitenkin ulkoistuksesta huolimatta yrityksellä itsellään. Myös ulkoistuskumppanien mahdollisista virheistä aiheutuneet muut haitat ja seuraamukset tulee ottaa huomioon.

Ulkoistuskumppanien kanssa tulee aikaansaada asianmukaiset sopimukset joissa sovitaan palveluista, tietoturvallisuudesta ja vastuista.

5.4 Organisaatio, vastuutus ja johtaminen

Yrityksen johdon tulee määrittää tavoiteltava tietoturvan taso ja huolehtia siitä, että käytettävissä on riittävät resurssit. Vastuu tietoturvallisuusasioista sekä tietoturvalisuuden toimeenpano tulee huomioida organisaatirakenteessa.

Testaus ja harjoittelu tulee olla suunnitelmallista ja jatkuvaa.

Johdon tulee myös vastata siitä, että tietoturvallisuusasiat ja kehittäminen ovat osana yrityksen taloudellista suunnittelua.

Tietoturvasta vastaavan henkilön tulee analysoida ja tunnistaa tietoturvariskit ja huolehtia siitä että riskien edellyttämät toimenpiteet on toteutettu.

5.5 Lainsäädännölliset vaatimukset

Koska kiinteistönvälitystoiminnan luonteeseen kuuluu kerää ja säilyttää ihmisten henkilötietoja tulee toiminnassa huomioida voimassaolevan lainsäädännön vaatimukset.

Henkilöstön sähköpostin käytöstä tulee laatia ohjeet ja sopia menettylystä kun työntekijä on estynyt itse käyttämästä sähköpostiaan tai työsuhde on päättynyt siten, että sovellatien lakien määräykset tulevat huomioiduiksi.

Lisäksi tulee seurata lainsäädännön kehitystä jotta järjestelmät ja käytänteet säilyvät lainmukaisina.

5.6 Koulutus

Tietoturvasta vastuussa olevan tulee huolehtia siitä, että tietoturvaa koskeva ohjeistus on lakien ja määräysten mukaisia.

Tietoturvasta vastaavan tulee huolehtia siitä, että yrityksen työntekijät saavat kattavan ohjeistuksen ja riittävästi koulutusta tietoturvaan liittyvissä asioissa. Työntekijöiden velvollisuutena on ymmärtää tietoturvan merkitys yritykselle ja sen liiketoiminnalle sekä noudattaa annettuja ohjeita.

5.7 Seuranta ja raportointi

Tietoturvan toteutumista tulee seurata järjestelmällisesti ja jatkuvasti. Tietoturvasta vastaavan tulee huolehtia siitä, että tietoturvan valvontaan on käytettävissä riittävät resurssit ja järjestelmät.

5.8 Seuraamukset laimilyönneistä

Tietoturvasta vastaavan henkilön tulee laatia esitys siitä kuinka tietoturvarikkomusten selvittely ja siitä seuraavat toimenpiteet järjestetään yrityksessä. Yhtiön hallitus kuitenkin tekee päätökset asiassa.

Koko henkilöstön tulee olla tietoisia tietoturvarikkomusten seuraamuksista.

5.9 Tietoturvapolitiikasta tiedottaminen

Henkilökunnalle, kumppaneille ja valikoiduille asiakkaille tiedotetaan yrityksen virallisesta tietoturvapolitiikasta.

5.10 Tietoturvapolitiikka-asiakirja

Suoritetun tutkimuksen tuloksena yrityksen tietoturvavastaava laati ehdotulksen yrityksen viralliseksi tietoturvapolitiikka-asiakirjaksi.

Liitteen A mukainen Tietoturvapolitiikka-asiakirja hyväksyttiin yhtiön hallituksen kokouksessa 17.5.2014.

6 Johtopäätökset ja loppusanat

Yrityksen tärkein tietoturvallisuutta koskeva dokumentti on tietoturvapolitiikka. Ilman sitä, yrityksen on vaikeaa ylläpitää haluttua tietoturvan tasoa, sekä sisällyttää se johdon strategisiin tavoitteisiin. Nykypäivänä tietotekniikka on osana yritysten jokapäiväistä toimintaa ja tietoturvan merkitys kasvaa entisestään. Jos yrityksen tietoturvantaso on heikko, niin riskit kasvavat entisestään. Maineen menetys, sekä taloudelliset haitat vaivaavat yrityksiä

jatkuvasti heikon tietoturvatason vuoksi, jossa joillekkin yrityksille se saattaa olla hyvinkin kohtalokasta. Yritysten johdon tulisi kiinnittää enemmän huomiota tietoturvallisuuteen kehittäessään omaa liiketoimintaansa, sekä ottamaan se osaksi strategista suunnittelua. Tietoturva-arkkitehti Kevin Pietersma, Toronton yliopistosta on sanonut seuraavasti: ”Information security is the immune system in the body of business”, joka vapaasti suomentaen kuuluu näin ”Tietoturva on koko liiketoiminnan immuunisysteemi”.

Välitysliikkeen hallitus on hyväksynyt tietoturvapolitiikan ja sen sisällön päivämäärällä 17.5.2014 ja kiittänyt opinnäytetyöntekijää vuoden kestävästä projektista. Tutkimuksen alkuvaiheessa oli haastavaa rajata työtä sopivaksi ja löytää konkreettinen ratkaisu tietoturvan kehittämiselle. Kun sopiva tutkimusongelma oli löydetty, työn rajaus helpottui myös merkittävästi. Konstruktiivinen tutkimusmenetelmä sopi tutkimustapana aiheeseen erittäin hyvin, sillä tavoitteena oli luoda jotakin uutta. Työn rajaus kuitenkin rajoitti konstruktiivisen tutkimuksen tulosten arviointia, sillä aika loppui kesken. Ojasalo & Co. Kuitenkin painottaa, että ratkaisun toimivuutta voidaan käytännössä arvioida joskus myöhemmin, sillä esteenä saattaa olla opinnäytetyön kiireellinen aikataulu.
Teoreettista tietoa löytyi hyvin paljon ja diversiteettia tietoa löytyi etenkin tietoturvan johtamisen eri tavoista. Aiheesta tietoturvapolitiikka, löytyy teoreettista tietoa hyvin paljon ja alan standardit erityisesti BSI-Grundschutz katalogi antoi hyvän järjestyksen, mitkä asiat tulivat ottaa huomioon ennen tietoturvapolitiikan laatimista. Erilaisista tietoturvapolitiikan malleista sai apua itse tietoturvapolitiikan luomiseen ja näkisin, että siitä oli myöskin apua havainnollistaessa asiaa yrityksen johdolle. Uskoisin, että välitysliike hyötyi projektista paljon, sillä yrityksen työntekijät ja johto saivat paljon sellaista tietoa mihin olisi mahdollisesti tarvittu ulkopuolisen konsultin apua. Yleisesti pienillä yrityksillä ei välttämättä ole yrityksen sisällä työntekijää jolla olisi aikaa paneutua asiaan ja tutkia aihetta näin laaja-alaisesti ja sen takia uskon, että tämä projektiluontoinen tapa lähestyä asiaa toimi erityisen hyvin. Oman näkemykseni mukaan yritys hyötyi projektista myös siten, että opinnäytetyön prosessin aikana tietoturvaa käsiteltiin hyvin laaja-alaisesti johdon kanssa käymissä palavereissa, niin samalla johdon tietoisuus myös strategisista asioista lisääntyi ja johto sanoi nähneensä tietoturva-asiat ”kokonaisuutena”, eikä pelkästään teknisistä asioista riippuvina. Varsinkin kun suurin osa teknisistä asioista olivat ulkoistettu.
Yrityksen tulee silti hyvällä seurannalla jatkaa tietoturvan kehittämistä jotta tietoturvan taso säilyisi hyvänä. Sillä siihen vaikuttavat niin sisäiset- kuin ulkoiset tekijät.

Näkisin, että tätä tutkimuksessa käytettyä prosessia voisi soveltaa yleisluonteisesti myös monissa muissa pienyrityksissä. Vaikka yritysten strategiset tavoitteet ja liiketoimintaprosessit saattaisivat poiketa toisistaan huomattavasti, ne voidaan selvittää käyttämällä tässä tutkimuksessa käytettyjä menetelmiä. Uutuusarvon osoittamiseksi voitaisiin esimerkiksi teettää asiakaskysely, jossa kysyttäisiin asiakkaan mielipidettä siitä miten he

näkevät tietoturvan systemaattisen parantamisen suhteessa asiakastyytyväisyyteen. Näkisin, että se voisi luoda hetkittäistä kilpailuetua, sillä yksityisyysasiat ja tietosuojaan liittyvät seikat ovat tänä ’post Snowden’ aikana hyvinkin ajankohtaisia asioita, joita ihmiset osaavat arvostaa.

Lopuksi haluan kiittää välitysliikettä mahdollisuudesta kehittyä aiheessa joka itselleni ei ollut ennestään niin tuttua. Haluan myös kiittää isääni saamastani tuesta, sekä opinnäytetyön ohjaajaani antamastaan asiantuntijuudesta ja ohjauksesta.

7 Lähteet

Andreasson, A., Koivisto, J. 2013. Tietoturvaa toteuttamassa. Helsinki: Tietosanoma Oy.

BSI: IT-Grundschutz Catalogues 2005

Hakala, M., Vainio, M., Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Porvoo: Docendo Finland Oy.

ISF: Standard of good practice for information security. 2007.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Ohjeistus, toteutus ja lainsäädäntö. Helsinki: Edita Publishing Oy.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2009. Kehittämistyön menetelmä. Uudenlaista osaamista liiketoimintaan. Helsinki: WSOYpro Oy.

http://www.finlex.fi/fi/laki/ajantasa/1999/19990523#L3 haettu 18.1.2014

http://www.nativeintelligence.com/ni-free/awareness-slogans.asp haettu 23.5.2014

http://www.silverskin.com/research/Tietoturvan_johtaminen_syksy_2012.pdf haettu 12.5.2014

http://www.tietojesiturvaksi.fi/content/todentaminen-ja-kiistämättömyys haettu 13.5.2014

https://www.vahtiohje.fi/web/guest/602 haettu 10.3.2014

http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101028Ohjeti/name.jsp haettu 4.4.2014

Kuvat ja kuviot

Liitteet

Liite 1: Yrityksen X Tietoturvapolitiikka

PRIMA KIINTEISTÖT OY LKV:N TIETOTURVAPOLITIIKKA

Johdanto sekä strategiset tavoitteet

Tämän tietoturvapolitiikan tavoitteena on luoda suunta tietoturvan jatkuvalle kehittämiselle, sekä tietoisuuden lisäämiselle organisaatiossa. Prima on vastuussa omien sidosryhmiensä tyytyväisyydestä ja haluaa toimia lain määräämien velvoitteiden, sekä hyvän tietojenkäsittelytavan mukaisesti jossa otetaan huomioon henkilöiden yksityisyydensuoja.

Tietoturvapolitiikka tukee yrityksen tavoitetta tarjota laadukkaita palveluita asiakkailleen. Tavoitteena on pitää huoli siitä, että tieto ei tuhoudu, joudu vääriin käsiin ja järjestelmät pysyvät toiminnassa. Edellytyksenä tälle, Prima on luonut ohjeet työntekijöille, sekä motivoi ja kouluttaa henkilöstöä vuosittain. Tietoturvallisuutta toteutetaan ja kehitetään käyttäen riskien kannalta tarkoituksenmukaisia ja kustannustehokkaita ratkaisuja.

Tieto on Primalle tärkeää omaisuutta ja sitä tulee turvata koko organisaation osalta samalla lailla kuin muutakin yrityksen omaisuutta jotta vältyttäisiin mahdollisilta taloudellisilta vahingoilta, sekä maineen heikentymiseltä. Priman liiketoiminnassa luottamuksellisia tietoja käytetään vain sopimuksien, sekä lainsäädännön sallimiin tarkoituksiin. Turvausmekanismeihin lukeutuvat niin hallinnolliset kuin teknispainotteiset toimet joilla tietoa suojataan.

Tietoturvatavoitteet ja käytännöt

Tietoturvallisuudella tarkoitetaan kaikkien tietojen, riippumatta siitä missä muodossa ne esiintyvät, turvallista käsittelyä. Tietoturvallisuudella varmistetaan tietojen eheys, käytettävyys ja luottamuksellisuus.

Tietoturvallisuus koskee yrityksen jokaista työntekijää, toimintoa, palvelua, järjestelmää, tai päätelaitetta jossa yritykselle tärkeää tietoa kulkee. Keinot joilla tätä tietoa koitetaan suojata ovat ohjeistettuna yrityksen työntekijöille erilaisina käyttöohjeina, sekä vastuina. Yrityksellä on nimettynä tietohallintopäällikkö, joka vastaa yrityksen tietoturvasta ja sen teknisistä toimista. Prima ylläpitää sähköistä rekisteriä myynti- ja ostotoimeksiannoista ja teknisin menetelmin pitää huolen siitä, että tietojärjestelmät toimivat keskeytyksittä. Henkilöstö on velvollinen raportoimaan mahdolliset tietoturvauhat tietohallintopäällikölle.

Lainmukaisuus

Priman koko henkilöstö on vastuussa siitä, että yritys toimii lain määräämien velvoitteiden mukaisesti, sekä noudattaa hyvää tietojenkäsittelytapaa jokapäiväisissä rutiineissaan. Omien

asiakkaiden, sekä työntekijöidensä tietosuoja on yritykselle tärkeää ja siinä se noudattaa erityistä varovaisuutta. Jokaisen työntekijän vastuulla on tiedon huolellinen käsittely.

Jalkauttaminen

Jalkauttamisesta on vastuussa yrityksen johto ja tietohallintopäällikkö. He ovat vastuussa tieoturvaohjeiden laatimisesta, sekä näyttämällä omalla esimerkillään hyvää tietojenkäsittelytapaa muulle yrityksen henkilöstölle.

Yritys kouluttaa henkilöstöä tietoturvallisuus asioissa ja motivoi heitä oppimaan lisää. Oikeanlainen tietoturvakulttuurin luominen on tärkeä osa yrityksen tietoturvapolitiikkaa. Tietoturvaohjeistusta dokumentoidaan ja päivitetään tarpeen vaatiessa, sekä henkilökuntaa koulutetaan vastaamaan omien työtehtäviensä tietoturvallisesta toiminnasta jatkuvasti.

Yritys tekee aina kirjallisen sopimuksen yhteistyökumppaniensa kanssa, jossa se määrittelee tietoturvavastuut, sekä roolit. Mahdolliset tietoturvaloukkaukset osataan näin paremmin vastuuttaa.

Seuranta

Yritys kouluttaa jatkuvasti henkilöstöään tietoturvaansa nähden, sekä seuraa lain määräämiä velvoitteita tietoturvallisuuden lisäämiseksi. Tietoturvapolitiikka on osana yrityksen laatustrategiaa, jolla se takaa asiakkailleen laadukkaampia ja turvallisempia palveluita. Tämä tietoturvapolitiikka on voimassa toistaiseksi, ellei toisin sanota ja sen onnistumisen toteutumiseen ovat vastuussa koko yrityksen henkilöstö.

Hyväksytty 17.52014